

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT
for the
Western District of Wisconsin

In the Matter of the Search of
2806 Coolidge Street, Madison, WI

)
)
) Case No. 22-mj-67
)
)
)

SEALED

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following premises located in the Western District of Wisconsin.

See Attachment A.

The person or property to be searched, described above, is believed to conceal:

See Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the information described in Attachment B.

YOU ARE COMMANDED to execute this warrant on or before APRIL 11, 2023 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

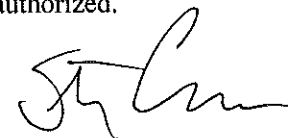
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Stephen L. Crocker.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for Days delayed days (not to exceed 30)
☐ until, the facts justifying, the later specific date of Date ending.

☐ Entry without knocking and announcing authority and purpose authorized.

Date and time issued:

7-28-23 AT 8:55 AM



Judge's signature

Madison, Wisconsin

Magistrate Judge Stephen L. Crocker

ATTACHMENT A

The property to be searched is 2806 Coolidge Street, City of Madison, Dane County, Wisconsin. It is a single story residential structure on the north side of Coolidge Street in the middle of the block between N Oak Street to the east and Kedzie Street to the west. The residence is finished with gray vinyl siding. The driveway to the residence is on the west side of the structure. There is a single car garage to the back of the property.



ATTACHMENT B

ITEMS TO BE SEIZED

1. All records, documents, programs, applications and information relating to violations of 18 U.S.C. § 844(1) (the Subject Offense), including, but not limited to:
 - a. Spray paint;
 - b. Mason jars;
 - c. Light jeans;
 - d. A black puffer jacket;
 - e. Black surgical masks;
 - f. All records, documents, programs, applications and information reflecting or relating to any intent, motive, or means of committing the Subject Offense;
 - g. All records, documents, programs, applications and information reflecting the intent or capacity to harm any person or carry out any threats against any person or property;
 - h. Training, instructional, and reference materials or other information, whether printed or in digital format, relating to Molotov cocktails;
 - i. Records, documents, programs, applications, personal notebooks, journals or materials relating to items listed above;
 - j. Any device that may be used to manufacture, compound, convert, produce, derive, process, or prepare, a Molotov cocktail;
 - k. Financial records, including bank account records, bank statements, deposit statements/slips, receipts, ledgers, cash receipt books, checks, checkbooks, canceled checks, check registers, withdrawal slips, Certificates of Deposits documents, wire transfers, cashier's checks, money orders, mutual fund and other securities' records, credit applications, loan documents, loan payments, loan statements, notes, invoices and/or bills, payroll records, billing information, safe deposit box records and keys;

1. Any digital device, including any digital device used to access the Internet and/or store Internet communications, such as central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices; and

m. Any electronic device used to facilitate the above-listed violations.

2. With respect to any electronic device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, monikers, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the presence or absence of computer software, hardware, or other application, which allows for anonymization of usage on a computer device, including Tor, Virtual Private Networks, VMWare, VirtualBox, multiple boot

capabilities, virtualization/virtual machine software, and drive cleaning/wiping software;

d. evidence of the presence or absence of encryption software, hardware, or other application;

e. any evidence of Internet research or communications regarding Molotov cocktails;

f. evidence of the attachment of other devices;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

h. evidence of the times the device was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the device;

j. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

k. records of or information about Internet Protocol addresses used by the device;

l. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. Any software, programs, or applications that can be used in the manipulation of data related to individual identifying information, stolen access device information, financial information, or account identifiers that can be encoded on the magnetic stripe of a credit card; and

n. Any records relating to electronic communications and/or other correspondence regarding access device fraud, including any stored or deleted communications.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

UNITED STATES DISTRICT COURT

for the
Western District of Wisconsin

In the Matter of the Search of
2806 Coolidge Street, Madison, WI

Case No. 22-mj-67

SEALED

APPLICATION FOR A SEARCH WARRANT

I, Elizabeth Altman, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following premises:
See Attachment A.

located in the Western District of Wisconsin, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 USC § 844(i)	Causing damage by fire or an explosive

The application is based on these facts: See attached Affidavit.

☐ Delayed notice of Days delayed days (give exact ending date if more than 30 days: Date ending) is requested under 18 U.S.C. § 3103a, the basis of which is set forth in the attached affidavit.

Sworn to before me telephonically on

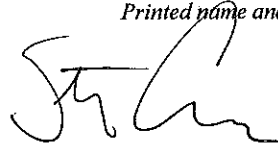
Date: 3-28-23

Madison, Wisconsin

Applicant's signature

Elizabeth Altman

Printed name and title

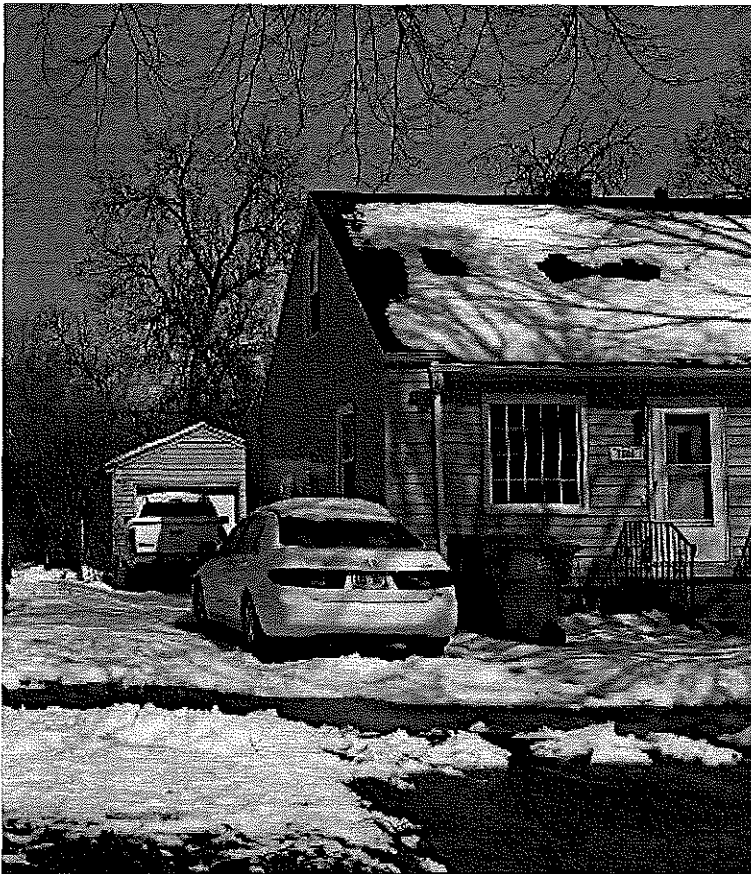


Judge's signature

Magistrate Judge Stephen L. Crocker

ATTACHMENT A

The property to be searched is 2806 Coolidge Street, City of Madison, Dane County, Wisconsin. It is a single story residential structure on the north side of Coolidge Street in the middle of the block between N Oak Street to the east and Kedzie Street to the west. The residence is finished with gray vinyl siding. The driveway to the residence is on the west side of the structure. There is a single car garage to the back of the property.



ATTACHMENT B

ITEMS TO BE SEIZED

1. All records, documents, programs, applications and information relating to violations of 18 U.S.C. § 844(1) (the Subject Offense), including, but not limited to:
 - a. Spray paint;
 - b. Mason jars;
 - c. Light jeans;
 - d. A black puffer jacket;
 - e. Black surgical masks;
 - f. All records, documents, programs, applications and information reflecting or relating to any intent, motive, or means of committing the Subject Offense;
 - g. All records, documents, programs, applications and information reflecting the intent or capacity to harm any person or carry out any threats against any person or property;
 - h. Training, instructional, and reference materials or other information, whether printed or in digital format, relating to Molotov cocktails;
 - i. Records, documents, programs, applications, personal notebooks, journals or materials relating to items listed above;
 - j. Any device that may be used to manufacture, compound, convert, produce, derive, process, or prepare, a Molotov cocktail;
 - k. Financial records, including bank account records, bank statements, deposit statements/slips, receipts, ledgers, cash receipt books, checks, checkbooks, canceled checks, check registers, withdrawal slips, Certificates of Deposits documents, wire transfers, cashier's checks, money orders, mutual fund and other securities' records, credit applications, loan documents, loan payments, loan statements, notes, invoices and/or bills, payroll records, billing information, safe deposit box records and keys;

1. Any digital device, including any digital device used to access the Internet and/or store Internet communications, such as central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices; and

m. Any electronic device used to facilitate the above-listed violations.

2. With respect to any electronic device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, monikers, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the presence or absence of computer software, hardware, or other application, which allows for anonymization of usage on a computer device, including Tor, Virtual Private Networks, VMWare, VirtualBox, multiple boot

capabilities, virtualization/virtual machine software, and drive cleaning/wiping software;

d. evidence of the presence or absence of encryption software, hardware, or other application;

e. any evidence of Internet research or communications regarding Molotov cocktails;

f. evidence of the attachment of other devices;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

h. evidence of the times the device was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the device;

j. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

k. records of or information about Internet Protocol addresses used by the device;

l. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. Any software, programs, or applications that can be used in the manipulation of data related to individual identifying information, stolen access device information, financial information, or account identifiers that can be encoded on the magnetic stripe of a credit card; and

n. Any records relating to electronic communications and/or other correspondence regarding access device fraud, including any stored or deleted communications.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.

STATE OF WISCONSIN)
) ss.
COUNTY OF DANE)

I, Cheryl Patty, being first duly sworn, hereby depose and state as follows:

1. I have been employed as a Wisconsin Law Enforcement Officer since November of 1995 as a Dane County deputy, and as a detective since June 2007. I have been assigned to the Federal Bureau of Investigation Madison Resident Agency as a Task Force Officer on the Joint Terrorism Task Force since May 2020. I have received basic law enforcement training and have attended numerous specialized law enforcement-training courses and schools, sponsored by the Wisconsin Department of Justice as well as other law enforcement agencies, relating to the investigation of a wide range of criminal activity. I have specialized training and experience including, but not limited to, homicide investigations, death investigations, fire investigations, sexual assault, stalking, domestic violence, battery, motor vehicle crashes, drug investigations, crimes against children, and other persons and property crimes. Over the course of numerous investigations, I have utilized data obtained through legal process related to cellular records, including location information. I have training and experience in interviewing witnesses and victims of crimes, developing and interviewing suspects and collecting and preserving physical evidence. These investigations often involve the forensic analysis of physical evidence.

2. In particular, I know the analysis of evidence for deoxyribonucleic acid (DNA) can play a critical role in these investigations. I have participated in dozens of

investigations in which DNA reference samples collected from suspects either voluntarily or through a search warrant were compared against DNA samples collected from physical evidence relevant to the cases. These comparisons can be of great value in either including or excluding suspects from cases but are not always dispositive on the issue of identification.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement agents, agencies, and witnesses. It does not set forth all my knowledge about this matter. It is merely intended to show probable cause that Hridindu Sankar ROYCHOWDHURY, and persons unknown to investigators, have committed violations of Title 18 U.S.C § 844(i), causing damage by fire or an explosive, and that there is probable cause to search the location 2806 Coolidge Street, Madison Wisconsin (the SUBJECT PREMESIS), further described in Attachment A, for evidence of that offense as further described in Attachment B.

PROBABLE CAUSE

4. On Sunday, May 8, 2022, at approximately 6:06 a.m., Madison Police Department police officers responded to an active fire at an office building located in Madison, Wisconsin. I know that the building is a multi-level office building located in an area consisting almost exclusively of commercial-use buildings.

5. The police responded to a 911 call from a civilian, who observed flames coming from a window.

6. Upon arrival at the location, the police observed a fire in an office on the Northwest corner of the building. On the north facing side of the building, the third window from the west end, facing the driveway, was broken. The police observed that inside the office, a row of books was lined up adjacent to the window and were smoking and burning with small flames. The police observed a mason jar directly under the area where the books were on fire. A red handkerchief was wrapped around the edge of the windowpane glass as if it was used to pry the broken glass from the window.

7. The police walked the perimeter of the building. On the west side, the police observed large black words spray painted in cursive style writing, "If abortions aren't safe then you aren't either." On the south facing wall of an alcove of the building, the police observed black spray painting with a large "A" with a circle around it and the number "1312."¹

8. Madison Fire Department responded, extinguished the fire, and gained access to the interior of the building. The police also went inside the building.

9. Once inside the building, the police observed the mason jar under the window; the jar was broken, and the lid and screw top were burned black. The police also saw a purple disposable lighter near the mason jar. On the opposite wall from the window, the police saw another mason jar with the lid on, and a blue cloth tucked into the screw top, with one edge slightly singed. The jar was about half full of a clear fluid

¹ I understand the large "A" with a circle around it represents an anarchist's symbol. I believe the "1312" represents the phrase "All Cops Are Bastards."

that smelled like an accelerant, possibly kerosene. A Special Agent/Certified Fire Investigator (SA/CFI) with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) later smelled the fluid and believed that it smelled like a flammable or combustible liquid.

10. The fire occurred in an office suite occupied by Organization A. The individual office affected by the fire belongs to the president of Organization A. Through this investigation, I have learned that Organization A maintains a website and uses social media to promote its goals.

11. The police spoke with the president of Organization A, who reported that while they previously received threats due to their positions on certain social issues, none of the threats were received over the last week. After the news of the potential Supreme Court decision in *Dobbs v. Jackson Women's Health Organization*, Organization A and its president have been vocal about their position on abortion rights. Organization A issued press releases and the president participated in interviews.

12. The ATF SA/CFI conducted an Origin and Cause investigation at the location, and the agent advised that the fire was caused by the application of an open flame to flammable/combustible vapors and was therefore classified as incendiary.

13. The ATF SA/CFI advised me that fire investigators collected a glass container with an attached fabric cloth, containing an unknown, clear liquid, consistent with the appearance and components of a Molotov cocktail, a breakable container, which contains a flammable/combustible liquid, and a wick. The devices are known

to investigators to have initiated fires. The contents were sent to the ATF laboratory for further analysis.

14. Preliminary ATF laboratory results from a forensic biologist show that the forensic biologist discovered DNA on multiple pieces of evidence suitable for further testing. The forensic biologist obtained DNA profiles from three different individuals. All the DNA profiles were located on evidence collected by investigators at the scene and sent to the ATF laboratory for analysis.

15. One DNA profile discovered during the forensic process indicates that a male profile, "Male 1," appears to be present on swabs from the top and bottom of the window glass, swabs from the exterior of the glass jar, swabs from the body of the lighter as well as swabs of the black and silver top of the lighter, including the ignition wheel and button of the lighter, and swabs from the exterior of the Molotov cocktail, and the blue cloth used in that Molotov cocktail.²

16. The ATF Laboratory submitted all the DNA profiles to the Combined DNA Index System (CODIS) to determine if the DNA profiles were already in the system. The search of CODIS returned no hits/matches.

17. On January 21, 2023, Wisconsin State Capitol Police were monitoring the Wisconsin State Capitol exterior cameras overseeing a planned protest related to an officer-involved shooting in Atlanta, Georgia. During the protest at the Wisconsin

² Additional DNA profiles were obtained from the scene and analyzed. Law enforcement has not yet been able to match them to a suspect.

State Capitol, law enforcement observed multiple individuals in various areas of the Capitol grounds spray painting graffiti.

18. On January 26, 2023, law enforcement continued to review surveillance camera footage from January 21, 2023, and observed two suspects, one who is seen spray painting "We will get revenge" with black spray paint in a cursive-style writing on the Capitol grounds. The message appeared to have some visual similarities to the graffiti left at Organization A; the comparisons have been sent to the FBI for analysis. The male believed to be ROYCHOWDHURY wore light jeans, a black puffer-type coat, and a black surgical mask.

19. On February 1, 2023, law enforcement conducted further review of surveillance camera footage from the Capitol exterior, and two suspects were observed arriving on the Capitol square at approximately 5:04 p.m. Law enforcement later observed the suspects leave the Capitol square at 5:25 p.m.

20. On February 3, 2023, law enforcement viewed surveillance footage for the Tenney Plaza Parking Ramp from January 21, 2023, from 4:55 p.m. to 7:05 p.m., to attempt to identify the men who spray painted the sidewalk at the Capitol. Law enforcement saw a white Toyota pickup truck enter the parking lot at 4:58 p.m. The vehicle had no front plate. Minutes later, at 5:03 p.m., law enforcement observed both suspects walk past the camera. At 6:54 p.m., law enforcement observed both suspects enter the parking ramp on foot, then walk out of camera view. At 6:58 p.m., law enforcement observed a white Toyota pickup truck leave the parking lot. That white pickup truck was a Toyota Tacoma and had a visible number on its rear license plate.

21. Law enforcement checks of the Wisconsin license plate returned to a white 2005 Toyota Tacoma pickup truck registered to Citizen 1 at the SUBJECT PREMESIS. Property records show Citizen 1 is the owner of this property.

22. On February 22, 2023, law enforcement located an Instagram post that posted the flyer for the Stop Cop City event at the Capitol on January 21, 2023. In the "likes" this post received, law enforcement saw the Instagram profile @Hridindu (Display name: Hridindu Roychowdhury).

23. According to DOT records, the SUBJECT PREMESIS is the address listed on ROYCHOWDHURY's driver's license. Additionally, in response to legal process, Experian Credit reported his current address as the SUBJECT PREMESIS.

24. On March 1, 2023, law enforcement observed the white Toyota Tacoma with the same license plate as was seen leaving the parking ramp being driven by an individual law enforcement believed was ROYCHOWDHURY. He was alone in the vehicle. Law enforcement saw the vehicle pull into the Dutch Mill Park and Ride parking lot located at 46 Collins Court, Madison, Wisconsin.

25. Law enforcement observed ROYCHOWDHURY park the vehicle in one of the vacant parking spots and remain parked for approximately 10-15 minutes. Law enforcement kept the vehicle in direct sight the entire time. At 3:40 p.m., law enforcement observed ROYCHOWDHURY step out of the driver's door of the vehicle. Law enforcement could see ROYCHOWDHURY clearly from their location, approximately 100 feet away. ROYCHOWDHURY's face was exposed and visible to law enforcement. Law enforcement identified the driver by comparing the person they

saw to ROYCHOWDHURY's Wisconsin driver's license photograph. After law enforcement observed ROYCHOWDHURY step out of the vehicle, law enforcement noticed him holding a brown fast food bag. Law enforcement saw ROYCHOWDHURY discard this bag on a pile of trash centered on a bin on a traffic island within the parking lot. Law enforcement then observed ROYCHOWDHURY get back into the vehicle and drive out of the parking lot.

26. Law enforcement had an unimpeded view of the brown paper bag ROYCHOWDHURY discarded. Law enforcement immediately walked up to the bin after ROYCHOWDHURY left the area. Law enforcement saw no other individuals near the bin, nor did law enforcement view anyone discard anything else in the bin between the time ROYCHOWDHURY discarded the brown paper bag to the point law enforcement walked up to it.

27. Law enforcement visually identified the bag as a fast food bag. The bag was crumpled shut near the top and appeared to have contents inside. Law enforcement further confirmed that this was the bag discarded by ROYCHOWDHURY because all the other trash beneath and surrounding it was water soaked from the precipitation earlier in the day. The fast food bag, however, was dry.

28. Law enforcement retrieved the bag from the trash. The contents of the bag included a quarter portion of a partially eaten burrito wrapped in waxed paper, a soiled napkin, a crumpled napkin, a stack of napkins, the wrapper of the burrito, a crumpled food wrapper, four unopened hot sauce packets, and the brown paper bag itself.

29. Law enforcement sent the collected evidence from the bag discarded by ROYCHOWDHURY to the ATF laboratory for analysis. Additionally, law enforcement swabbed the burrito for DNA and sent the swab to the ATF lab.

30. On March 17, 2023, the ATF laboratory advised that a forensic biologist with the ATF laboratory examined the evidence law enforcement submitted and located a DNA profile. The results from the ATF laboratory indicate the DNA collected from the contents of the brown paper bag is a match to the DNA of "Male 1" that was recovered from evidence at the arson that occurred at Organization A. Because the items were taken after ROYCHOWDHURY discarded them, I believe the DNA is his.

31. Within the last week, law enforcement learned that ROYCHOWDHURY purchased a one-way flight from Boston, Massachusetts, to Guatemala City, leaving on March 27, 2023. They also determined that he left Madison and flew to Portland, Maine, on March 23, 2023. Additionally, law enforcement determined that Citizen 1 flew from Madison to Guatemala City on January 18, 2023, and Citizen 1 has a return flight booked for September 17, 2023.

32. Even though ROYCHOWDHURY purchased a one-way flight, I believe it is likely the items listed in Attachment B will still be present at the SUBJECT PREMESIS. The location is his last known residence, and Citizen 1 is scheduled to return to the SUBJECT PREMISES in September 2023. The defendant was arrested on March 28, 2003, when he arrived at the airport for his flight to Guatemala. He had one checked suitcase, one carry-on bag, and one backpack. Therefore, it is more likely

than not that ROYCHOWDHURY left belongings that he did not take with him to Guatemala at the residence. Those items are likely to include electronic items, cold-weather clothing as seen in the video of him at the Capitol, masks, and spray-paint cans. In addition to evidence implicating ROYCHOWDHURY in the crime, items left in the home, especially electronic items, are likely to help identify the other people involved in the offense.

33. At this time, it is unknown who, if anyone is residing at the SUBJECT PREMESIS, or who may have electronic devices stored there. If law enforcement is unable to determine which devices belong to ROYCHOWDHURY, this warrant seeks permission to seize and search all electronic devices. If it becomes clear during analysis that a device does not belong to ROYCHOWDHURY, agents will stop their search immediately.

COMPUTER AND ELECTRONIC EVIDENCE

34. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, other storage media, or within a hand-held electronic device such as a cellular telephone or personal digital assistant (e.g., iPod Touch or iPad devices). Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

TECHNICAL TERMS

35. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. The Internet Protocol address (or simply "IP address") is a unique numeric address used by internet-enabled electronic storage devices. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. "Cellular telephone" or "cell phone" means a hand held wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications,

wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

d. "Computer," is defined in 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

e. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices such as, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices; peripheral input/output devices such as, keyboards, printers, video display monitors, and related communications devices such as cables and connections; and any devices, mechanisms, or parts that can be used to restrict access to computer hardware such as, physical keys and locks.

f. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, or hide protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form such as, writings or drawings; photographic form such as prints, negatives, videotapes, motion pictures, or photocopies; mechanical form such as printing or typing; or electrical, electronic or magnetic form such as tape recordings,

cassettes, compact discs, hard drives, Personal Digital Assistants, Multi Media Cards, USB devices, smart cards, and memory calculators, as well as printouts or readouts from any magnetic, electrical or electronic storage device.

j. "Electronic storage devices" includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB "thumb drives"). Many of these devices also permit users to communicate electronic information through the internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

36. Based on my training and experience, I know that in order to properly retrieve and analyze electronically stored (computer) data, and to insure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the electronic storage devices. To effect such accuracy and completeness, it may also be necessary to analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, other storage media, within a hand-held electronic

device such as a cellular telephone or a tablet device (e.g., an iPad device). Some of these electronic information, as explained below, might take a form that becomes meaningful only upon forensic analysis.

37. I submit that if a computer or other electronic storage device is found on the premises, there is probable cause to believe those records will be stored in that electronic storage device, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on an electronic storage device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. It follows that deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone, or tablet device) the device may also contain a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, electronic storage device storage media-in particular, computers' internal hard drives-contain electronic evidence

of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, and file system data structures. Electronic storage device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

38. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how electronic storage devices were used, the purpose of their use, who used them, and when.

39. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), electronic storage device storage media can contain other forms of electronic evidence as described below:

a. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been

deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within an electronic storage device and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an electronic storage device (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic storage device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic storage device was remotely accessed, thus inculcating or exculpating the electronic storage device owner. Further, electronic storage device activity can indicate how and when

the electronic storage device was accessed or used. For example, as described herein, computers typically contain information that log computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera). The geographic and timeline information described herein may either inculcate or exculpate the electronic storage device user. Last, information stored within an electronic storage device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic storage device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user's knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner.

40. Based upon my knowledge, training, and experience, I know that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some electronic storage device equipment,

peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

- a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how an electronic storage device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.
- b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.
- c. Technical requirements. Electronic storage devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of electronic storage device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

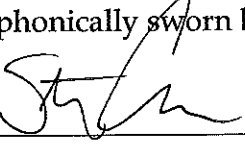
41. In light of these concerns, I hereby request the Court's permission to seize the electronic storage devices, associated storage media, and associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the hardware, media, or peripherals on-site for this evidence.

CONCLUSION

42. I submit that this affidavit supports probable cause for a warrant to search the premises described in Attachment A and seize the items described in Attachment B.

Cheryl Patty
Detective, Dane County Sheriff's Office
Task Force Officer, Federal Bureau of
Investigation

Telephonically sworn before me this 28th day of March 2023.



Honorable STEPHEN L. CROCKER
United States Magistrate Judge

ATTACHMENT A

The property to be searched is 2806 Coolidge Street, City of Madison, Dane County, Wisconsin. It is a single story residential structure on the north side of Coolidge Street in the middle of the block between N Oak Street to the east and Kedzie Street to the west. The residence is finished with gray vinyl siding. The driveway to the residence is on the west side of the structure. There is a single car garage to the back of the property.



ATTACHMENT B

ITEMS TO BE SEIZED

1. All records, documents, programs, applications and information relating to violations of 18 U.S.C. § 844(1) (the Subject Offense), including, but not limited to:
 - a. Spray paint;
 - b. Mason jars;
 - c. Light jeans;
 - d. A black puffer jacket;
 - e. Black surgical masks;
 - f. All records, documents, programs, applications and information reflecting or relating to any intent, motive, or means of committing the Subject Offense;
 - g. All records, documents, programs, applications and information reflecting the intent or capacity to harm any person or carry out any threats against any person or property;
 - h. Training, instructional, and reference materials or other information, whether printed or in digital format, relating to Molotov cocktails;
 - i. Records, documents, programs, applications, personal notebooks, journals or materials relating to items listed above;
 - j. Any device that may be used to manufacture, compound, convert, produce, derive, process, or prepare, a Molotov cocktail;
 - k. Financial records, including bank account records, bank statements, deposit statements/slips, receipts, ledgers, cash receipt books, checks, checkbooks, canceled checks, check registers, withdrawal slips, Certificates of Deposits documents, wire transfers, cashier's checks, money orders, mutual fund and other securities' records, credit applications, loan documents, loan payments, loan statements, notes, invoices and/or bills, payroll records, billing information, safe deposit box records and keys;

1. Any digital device, including any digital device used to access the Internet and/or store Internet communications, such as central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices; and

m. Any electronic device used to facilitate the above-listed violations.

2. With respect to any electronic device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, monikers, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the presence or absence of computer software, hardware, or other application, which allows for anonymization of usage on a computer device, including Tor, Virtual Private Networks, VMWare, VirtualBox, multiple boot

capabilities, virtualization/virtual machine software, and drive cleaning/wiping software;

d. evidence of the presence or absence of encryption software, hardware, or other application;

e. any evidence of Internet research or communications regarding Molotov cocktails;

f. evidence of the attachment of other devices;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

h. evidence of the times the device was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the device;

j. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

k. records of or information about Internet Protocol addresses used by the device;

l. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. Any software, programs, or applications that can be used in the manipulation of data related to individual identifying information, stolen access device information, financial information, or account identifiers that can be encoded on the magnetic stripe of a credit card; and

n. Any records relating to electronic communications and/or other correspondence regarding access device fraud, including any stored or deleted communications.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.